Hastings International and Comparative Law Review

Volume 25
Number 2 *Spring 2002*

Article 4

1-1-2002

Electronic Signatures: A Comparison of American and European Legislation

Lance C. Ching

Electronic Signatures: A Comparison of American and European Legislation

BY LANCE C. CHING*

Introduction

The federal Electronic Signatures in Global and National Commerce Act (Electronic Signatures Act) became effective on October 1, 2000.[1] The purpose of this Act is to establish that a signature, contract, or record related to an interstate or foreign transaction cannot be denied legal effect simply because it is in electronic form, subject to certain exceptions. For much the same purpose, the European Parliament and Council adopted the Directive on a Community Framework for Electronic Signatures (Electronic Signatures Directive) in December 1999.[2]

This Note will discuss the approaches taken by the United States and the European Union to establishing the validity of electronic signatures. Part I provides a brief overview of the history of electronic commerce and legislation intended to promote its development. Part II discusses the current and proposed legislation of the United States. Part III discusses the current and proposed legislation of the European Union. Part IV compares the two models, focusing on areas where the two approaches differ and discussing the relative strengths and weaknesses of both.

I. Development of Electronic Commerce Legislation

The Internet is the fastest growing medium in the history of

* J.D. candidate, University of California, Hastings College of the Law, 2002.

1. Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229, 114 Stat. 464 (2000) [hereinafter Electronic Signatures Act].

2. Council Directive 99/93/EC, 2000 O.J. (L 13) 12 [hereinafter Electronic Signatures Directive].

telecommunications.[3] In 1994, three million people, mostly in the United States, were using the Internet.[4] By 1998, 100 million people were using the Internet worldwide.[5] In comparison, radio was in use for thirty-eight years before it had fifty million users, and it took television thirteen years before it reached fifty million viewers.[6]

During the mid-1990's, businesses began to use the Internet to conduct commercial transactions with their business partners.[7] This form of electronic commerce has grown rapidly over the past few years; resulting in over $150 billion in revenues in 1999.[8] By the year 2003, electronic commerce could account for over $3 trillion in revenues.[9]

Not surprisingly, governments around the world have welcomed electronic commerce and its attendant economic benefits, and encouraged its further development. Despite this widespread support, a certain degree of uncertainty has always remained regarding the legal validity of electronic commerce. Part of this uncertainty is based on the fact that the statutes of many states and countries require certain contracts to be in writing and signed by the contracting parties. The Statute of Frauds is an example of such a writing requirement.[10] The question thus posed by such writing requirements is, can a contract that has been created in electronic rather than written form be considered legally enforceable? Also, more specifically, can an electronic signature fulfill the same requirements as a written signature?

In order to avoid such uncertainty, the early participants in electronic commerce were forced to enter into preliminary trading partner agreements.[11] These agreements stipulated in advance the parties' desire that their subsequent electronic communications should be given legal effect.[12] Of course, the preliminary agreements

3. U.S. DEP'T OF COMMERCE, THE EMERGING DIGITAL ECONOMY (1998). The Internet is a global matrix of interconnected computer networks using the Internet Protocol to communicate with each other. Id. at 1.

4. *Id* at 7.

5. *Id.*

6. *Id.* at 4.

7. *Id.*

8. John Peet, *Shopping Around the Web*, THE ECONOMIST, Feb. 26, 2000, at 5.

9. *Id.*

10. *See* U.C.C. § 2-201(1) (1998).

11. *See* Robert A. Wittie & Jane K. Winn, *Electronic Records and Signatures Under the Federal E-Sign Legislation and the UETA*, 56 BUS. LAW. 293, 294 (2000).

12. *See id.*

themselves had to be in writing and authenticated by a handwritten signature.[13] Thus, while these agreements had the limited effect of reducing uncertainty for the contracting parties, they had no effect on the validity of electronic commerce in general.

Addressing this lingering uncertainty, a 1995 U.S. government report described the relationship between contract law and electronic commerce:

> The challenge for commercial law [is] to adapt to the reality of the NII [National Information Infrastructure] by providing clear guidance as to the rights and responsibilities of those using the NII. Without certainty in electronic contracting, the NII will not fulfill its commercial potential. [Regardless] of the type of transaction, where parties wish to contract electronically, they should be able to form a valid contract online. In particular, online licenses should be encouraged because they offer efficiency for both licensors and licensees.[14]

As this suggests, by the mid-1990s, there was a general consensus that the validity of electronic commerce should be recognized.[15] By the year 2000, forty-nine states, the U.S. federal government, and the governments of over fifteen countries had either adopted or were considering some form of electronic commerce legislation.[16] Much of this legislation focused on the validity of electronic signatures.[17]

Unfortunately, while there was a general consensus that electronic signatures should be accorded the same validity as handwritten signatures, there was little agreement on how to achieve this goal.[18] The procedures chosen by the various governments differed greatly on a number of points.[19] Some governments chose to authorize electronic signatures under limited circumstances, other governments chose to create systems of evidentiary presumptions and default provisions that parties could contract out of, while other governments chose highly regulatory approaches that promoted

13. *See id.*

14. Raymond T. Nimmer, *Electronic Signatures and Records: The New U.S. Perspective*, 17 COMPUTER & INTERNET LAW. 8, 8 (2000).

15. *See id.*

16. Thomas J. Smedinghoff & Ruth Hill Bro, *Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce*, 600 PLI/PAT 507, 512 (2000).

17. *See id.*

18. *Id.* at 513.

19. *See id.*

certain technologies and employed rigid certification requirements.[20]

This variance in regulations has created a situation where the laws of one jurisdiction are often at odds with those of another making it increasingly difficult and costly for businesses to determine which jurisdiction's regulatory scheme will be applicable to them.[21] Transaction costs rise as parties are compelled to investigate the regulations of every state or country with which their online concern might conceivably do business.[22] An unfortunate result of this wave of incompatible legislation is that businesses are left with as much uncertainty regarding the legality of electronic commerce as they had before.[23] In a report discussing the difficulties of promoting the development of global electronic commerce, the Organisation for Economic Co-operation and Development (OECD) stated:

> The inherently global nature of today's network environment challenges the ability of national governments to address these issues on their own. In fact, unco-ordinated, inconsistent national policies for electronic commerce, no matter how well-intentioned, could be worse than no action at all, and it is generally agreed that an internationally co-ordinated approach is needed.[24]

In an effort to harmonize the disparate laws of their member states and to promote a more unified system of global electronic commerce, both the United States and the European Union sought guidance from a model provided by the United Nations Commission on International Trade Law (UNCITRAL).[25] The UNCITRAL Model Law on Electronic Commerce was drafted in 1996 for the purpose of encouraging state and national governments to enact electronic commerce regulations based on uniform principles.[26]

---

20. *See id.*

21. *See* Amelia H. Boss, *Searching for Security in the Law of Electronic Commerce*, 588 PLI/PAT 401, 422-26 (2000).

22. *See* Mark Owen, *International Ramifications of Doing Business Online: Europe*, 611 PLI/PAT 685, 694 (2000).

23. *See* Boss, *supra* note 21, at 422-26.

24. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, DISMANTLING THE BARRIERS TO GLOBAL ELECTRONIC COMMERCE (1997).

25. *See* Christina Hultmark, *European and U.S. Perspectives on Electronic Documents and Electronic Signatures*, 14 TUL. EUR. & CIV. L.F. 123, 130-31 (1999).

26. *See* UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, G.A. Res. 51/162, U.N. GOAR, 85th mtg., U.N. Doc. A/CN.9/SER.A/1996 *available at* http://www.uncitral.org/english/texts/electcom/ml-ec.htm (last visited Feb 10, 2002).

II. Legislative Approach of the United States

A. *State Legislation*

In 1995, Utah became the first state to enact some form of electronic signature legislation.[27] The Utah Digital Signature Act focused solely on a form of electronic signature that employed cryptographic technology to insure security.[28] Later, California became the second state to enact electronic signature legislation.[29] However, California took a more technology-neutral approach to its legislation, not mandating any particular form of technology.[30] Soon thereafter, the majority of states began to enact electronic signature legislation of their own, creating a patchwork of various regimes and requirements throughout the nation.[31] In the face of the rapid growth of electronic commerce, predictability regarding online transactions between jurisdictions soon became a difficult prospect.[32]

B. *Proposed Uniform Laws*

In an effort to promote greater uniformity between the various state regulations, the National Conference of Commissioners on Uniform State Laws (NCCUSL) approved the Uniform Electronic Transactions Act (UETA) and the Uniform Computer Information Transactions Act (UCITA) in July 1999, for adoption by the states.[33] Drafted to conform to the UNCITRAL Model Law on Electronic Commerce, the purpose of these acts is to establish legal recognition of electronic signatures, electronic records, and electronically-created contracts, under state law.[34] UCITA sets forth procedural and substantive rules that address the uncertainty regarding contractual relationships in transactions that involve the licensing of computer information, while UETA modifies state laws regarding writing and

27. *See* Smedinghoff & Bro, *supra* note 16, at 512.
28. *See* UTAH CODE ANN. §§ 46-3-101 to 46-3-504 (1999).
29. *See* Smedinghoff & Bro, *supra* note 16, at 512.
30. *See* CAL. GOV'T CODE § 16.5 (West 1999).
31. *See* Smedinghoff & Bro, *supra* note 16, at 512.
32. *See* Wittie & Winn, *supra* note 11, at 295-96.
33. *See* Nimmer, *supra* note 14, at 8.
34. *See* Mary Jo Dively, *The New Laws That Will Enable Electronic Contracting: Survey of Electronic Contracting Rules in the Uniform Electronic Transactions Act and the Uniform Computer Information Transactions Act*, 644 PLI/PAT. 159, 163-65, 174-75 (2001).

signature requirements.[35] As of July 18, 2001, UETA has been enacted by thirty-seven state legislatures and is pending in seventeen others.[36]

C. The Electronic Signatures Act

Congress enacted the Electronic Signatures Act on June 30, 2000, as an interim measure to insure that each state will recognize the validity of electronic signatures until such time as all states have adopted UETA.[37] While not as broad as UETA on a number of points, the Electronic Signatures Act preempts state laws that deviate significantly from the principles set forth by UETA.[38]

The Electronic Signatures Act is made up of four titles. Title I establishes fundamental rules governing the use of electronic signatures and records.[39] Title II sets forth provisions for the recognition of electronic negotiable instruments, or "transferable records."[40] Title III encourages the international recognition of electronic signatures and records.[41] Title IV makes a minor amendment to the Child Online Protection Act.[42]

The general principle of the Electronic Signatures Act is simple: any requirement that a contract be signed or that a document be in writing can be satisfied by an electronic signature or an electronic record.[43] Section 101(a) of the Electronic Signatures Act states:

> Notwithstanding any statute, regulation, or other rule of law... with respect to any transaction in or affecting interstate or foreign commerce—
>
> (1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
>
> (2) a contract relating to such transaction may not be denied legal

35. *See* Nimmer, *supra* note 14, at 8.

36. *See* Baker & McKenzie, Global E-Commerce Law Website, *at* http://www.bmck.com/ecommerce/vetacomp.htm (last visited Feb 5, 2002).

37. *See* Wittie & Winn, *supra* note 11, at 296-97.

38. *See* Nancy L. Perkins, *New Electronic Signature Legislation Validates Online Contracting*, 17 COMPUTER & INTERNET LAW. 1, 2 (2000).

39. *See* Electronic Signatures Act, *supra* note 1, §§ 101-107.

40. *See id.* §§ 201-202.

41. *See id.* § 301.

42. *See id.* § 401.

43. *See* Nimmer, *supra* note 14, at 9.

> effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.[44]

Section 106 of the Electronic Signatures Act defines the terms "electronic signature" and "record" broadly.[45] Laws that require a contract to be signed are generally interpreted by the Electronic Signatures Act as requiring "authentication."[46] An "electronic signature" is defined as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."[47] Since the intent to sign the record is a key component of this definition, electronic signatures are able to provide authentication.[48] Laws that refer to a "writing" are interpreted as referring to a "record."[49] A "record" is defined as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form."[50]

1. Consumer Protection

A great deal of Title I is devoted to the protection of consumers' rights.[51] It should be noted that while the Electronic Signatures Act goes far to ensure the validity of electronic signatures, it does not *require* people to use electronic signatures.[52] A key requirement of the Electronic Signatures Act is that consumers must give their consent to conduct transactions electronically before electronic records can be used as a substitute for traditional written records.[53]

In order for electronic records to fulfill writing requirements, Section 101(c)(1) requires that:

> A. the consumer has affirmatively consented to such use and has not withdrawn such consent;
>
> B. the consumer, prior to consenting, is provided with a clear and conspicuous statement—

44. Electronic Signatures Act, *supra* note 1, § 101(a).
45. *See* Nimmer, *supra* note 14, at 14.
46. *See id.*
47. Electronic Signatures Act, *supra* note 1, § 106(5).
48. *See* Nimmer, *supra* note 14, at 14.
49. *See id.*
50. Electronic Signatures Act, *supra* note 1, § 106(9).
51. *See* Perkins, *supra* note 38, at 2.
52. *See id.*
53. *See* Electronic Signatures Act, *supra* note 1, § 101(c)(1).

> i. informing the consumer of (I) any right or option of the consumer to have the record provided or made available on paper or in nonelectronic form, and (II) the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any conditions, consequences (which may include termination of the parties' relationship), or fees in the event of such withdrawal . . . .[54]

The consumer must also be provided with a statement regarding the hardware and software requirements for access to and retention of the electronic records.[55] Additionally, the consumer must be given information regarding how, after consenting, he or she may obtain a paper copy of the electronic statement, and whether a fee will be charged for the service.[56] Further, the consumer must be given a description of the procedures necessary to withdraw his or her consent.[57] Finally, Section 101(c)(1)(C)(ii) requires that the consumer either consent or confirm his or her consent electronically, "in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent."[58]

In order to ensure that the consumer is not harmed by changing technologies, Section 101(c)(1)(D) requires that the consumer be provided with a statement explaining new hardware and software requirements if, after the consumer provides consent, there is a change in the hardware or software requirements needed to access or retain electronic records such that there is a material risk that the consumer will not be able to access or retain an electronic record that was the subject of the consent.[59] Further, the consumer must be given the right to withdraw his or her consent without the imposition of any fees for such withdrawal, and without the imposition of any condition or consequence that had not been initially disclosed.[60]

While the Electronic Signatures Act allows a consumer to withdraw his or her consent, it does not allow the consumer to do so in a way that arbitrarily harms parties that have acted in reliance on

54. *Id.* § 101(c)(1)(A), (B)(i).
55. *Id.* § 101(c)(1)(C)(i).
56. *Id.* § 101(c)(1)(B)(iv).
57. *Id.* § 101(c)(1)(B)(iii).
58. *Id.* § 101(c)(1)(C)(ii).
59. *Id.* § 101(c)(1)(D).
60. *Id.* § 101(c)(1)(D)(i).

that consent.[61] Withdrawal of consent has a prospective rather than a retroactive effect.[62] Therefore, the validity and enforceability of electronic records that were provided or made available to the consumer before withdrawal would not be affected.[63]

2. Preemption of State Laws

As stated earlier, the Electronic Signatures Act was enacted as an interim measure to give state legislatures sufficient time to incorporate UETA. With this purpose in mind, Section 102(a) provides the states with a way to "opt out" of the Electronic Signatures Act.[64] A state legislature can enact statutes or regulations that modify, limit, or supercede the Electronic Signatures Act if the state adopts the UETA as recommended by the NCCUSL.[65] Alternatively, the state could specify "alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures" so long as (1) the alternative procedures or requirements are consistent with the principles of the Electronic Signatures Act, and (2) such alternative procedures or requirements do not "require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures."[66] The purpose of this second requirement is to ensure that a state does not confer a benefit or impose a burden on the use of a particular technology.[67]

3. Specific Exclusions

The Electronic Signatures Act does not apply to certain documents. According to Section 103(a):

> The provisions of section 101 shall not apply to a contract or other record to the extent it is governed by—
>
> (1) a statute, regulation, or other rule of law governing the creation and execution of wills, codicils, or testamentary trusts;

61. *See* Perkins, *supra* note 38, at 3.
62. *See* Electronic Signatures Act, *supra* note 1, § 101(c)(4).
63. *See id.*
64. *See id.* § 102(a).
65. *Id.* § 102(a)(1).
66. *Id.* § 102 (a)(2).
67. *See* Perkins, *supra* note 38, at 4.

(2) a State statute, regulation, or other rule of law governing adoption, divorce, or other matters of family law; or

(3) the Uniform Commercial Code, as in effect in any State, other than sections 1-107 and 1-206 and Articles 2 and 2A.[68]

Section 103(b) also excludes the following documents from the Electronic Signatures Act:

(1) court orders or notices, or official court documents (including briefs, pleadings, and other writings) required to be executed in connection with court proceedings;

(2) any notice of—

A. the cancellation or termination of utility services (including water, heat, and power);

B. default, acceleration, repossession, foreclosure, or eviction, or the right to cure, under a credit agreement secured by, or a rental agency for, a primary residence of an individual;

C. the cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities); or

D. recall of a product, or material failure of a product, that risks endangering health or safety; or

(3) any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.[69]

4. Applicability to the Federal and State Governments

Section 104 is written to provide flexibility to the federal and state governments, allowing them, under certain circumstances, to require that signatures or records continue to be made or retained in written form.[70] Federal and state regulatory agencies that are responsible for rulemaking under any other statute have the authority to interpret the basic rule of the Electronic Signatures Act with respect to such statute through:

(1) the issuance of regulations pursuant to a statute; or

68. Electronic Signatures Act, *supra* note 1, § 103(a),
69. *Id.* § 103(b).
70. *See* Perkins, *supra* note 38, at 5.

(2) to the extent that such agency is authorized by statute to issue orders or guidance, the issuance of orders or guidance of general applicability that are publicly available and published . . . .[71]

Section 104(b)(2) imposes limitations on these agencies' interpretive authority.[72] Any interpretive regulations, orders, or guidance must be consistent with section 101, must not add any requirements to section 101, and there must be "a substantial justification for the regulation, order, or guidance."[73] Also, the methods selected to carry out that purpose must be substantially equivalent to the requirements imposed on non-electronic records, and must not impose unreasonable costs on the acceptance and use of electronic records.[74]

Section 104(b)(2)(C)(iii) also requires that these methods be technology-neutral, not conferring a benefit or imposing a burden on a particular technology.[75] However, this general technology neutrality provision can be overridden by section 104(b)(3) if the promotion of a particular technology is necessary to assure the accuracy, record integrity, and accessibility of records that must be retained.[76]

5. Transferable Records

Title II of the Electronic Signatures Act sets forth a number of provisions intended to promote the establishment of a uniform national standard for the creation, recognition, and enforcement of "transferable records."[77] Under these provisions, transferable records, which are defined as electronic records that would be promissory notes or documents if they were in written form, may be executed using an electronic signature.[78]

6. Promotion of International Electronic Commerce

Title III of the Electronic Signatures Act sets forth provisions intended to encourage the international recognition of electronic

71. Electronic Signatures Act, *supra* note 1, § 104(b)(1).
72. *See id.* § 104(b)(2).
73. *Id.* § 104(b)(2)(A)-(C)(i).
74. *Id.* § 104(b)(2)(C)(ii).
75. *Id.* § 104(b)(2)(C)(iii).
76. *See id.* § 104(b)(3)(A).
77. *See* Perkins, *supra* note 38, at 6.
78. *See id.*

signatures and records.[79] These provisions direct the Secretary of Commerce to take all necessary actions to promote the use and acceptance of electronic signatures and records in interstate and foreign commerce.[80] Section 301(a)(2) establishes a number of principles to be followed in the course of such promotion:

A. Remove paper-based obstacles to electronic transactions by adopting relevant principles from the Model Law on Electronic Commerce adopted in 1996 by the United Nations Commission on International Trade Law.

B. Permit parties to a transaction to determine the appropriate authentication technologies and implementation models for their transactions, with assurance that those technologies and implementation models will be recognized and enforced.

C. Permit parties to a transaction to have the opportunity to prove in court or other proceedings that their authentication approaches and their transactions are valid.

D. Take a nondiscriminatory approach to electronic signatures and authentication methods from other jurisdictions.[81]

7. Studies

The Electronic Signatures Act requires two federal agency studies.[82] First, the Secretary of Commerce must conduct an inquiry of the effectiveness of the delivery of electronic records to consumers using electronic mail, compared with delivery of written records via the U.S. Postal Service.[83] Second, the Secretary of Commerce and the Federal Trade Commission must submit a report to Congress that analyzes the following:

- The benefits provided to consumers by the consumer access test of the consent provision (section 101(c)(1)(C)(ii));
- Any burdens imposed on electronic commerce by the provision;
- Whether the benefits outweigh the burdens; and
- Whether the absence of such procedure would increase

79. *See* Electronic Signatures Act, *supra* note 1, § 301(a).
80. *Id.* § 301(a)(1).
81. *Id.* § 301(a)(2).
82. *See id.* § 105.
83. *See id.* § 105(a).

consumer fraud.[84]

In conducting this evaluation, these agencies are to solicit comments from the general public, consumer representatives, and electronic commerce businesses.[85]

In June 2001, the Federal Trade Commission and the Department of Commerce submitted a report to Congress, indicating that the benefits provided by the consumer access test and consent provision outweighed any burdens imposed, and recommending no amendment to the provision.[86]

III. Legislative Approach of the European Union

During 1997, Germany and Italy became the first Member States of the European Union to enact electronic signature legislation.[87] In response to the rapid growth of online transactions, several other Member States began to draft similar legislation.[88] It soon became apparent, however, that the approaches taken by these Member States were diverse and potentially incompatible with one another.[89]

On October 8, 1997, the European Commission submitted a report to the European Parliament and Council, recommending the development of a European framework for electronic signatures.[90]

In response to this report, the Council invited the Commission to submit a directive on electronic signatures.[91] After consulting with the Member States, the Commission delivered an initial proposal on May 13, 1998.[92] On January 13, 1999, the European Parliament completed its first reading of the proposal.[93] An amended proposal was submitted on April 29, 1999.[94] The European Parliament

84. Perkins, *supra* note 38, at 7; Electronic Signatures Act, *supra* note 1, § 105(b).

85. *See* Electronic Signatures Act, *supra* note 1, § 105(b).

86. *See* Jeffrey P. Cunard & Jennifer B. Coplan, *Developments in Internet and E-Commerce Law: 2001*, 678 PLI/PAT. 935, 1051 (2001).

87. *See* Anthony Burke, *EU and Irish Internet Law: An Overview*, 13-AUT INT'L L. PRACTICUM 107, 113-115 (2000).

88. *See id.* at 113-16.

89. *See* Miriam A. Parmentier, *Electronic Signatures*, 6 COLUM. J. EUR. L. 251, 252 (2000).

90. *See id.*

91. *See* Michael L. Michael & Xiomara Corral, *Electronic Signatures: The European Perspective*, 4 WALLSTREETLAWYER.COM: SEC. ELEC. AGE 25 (2000).

92. Parmentier, *supra* note 89, at 252.

93. *Id.*

94. *Id.*

completed its second reading of the proposal on October 27, 1999.[95] Finally, on December 13, 1999, the European Parliament and Council adopted the Directive on a Community Framework for Electronic Signatures (Electronic Signatures Directive).[96]

Written to facilitate the use of electronic signatures, the Electronic Signatures Directive is part of a series of directives intended to promote the development of electronic commerce.[97] Included in this series of directives are the Directive on the Protection of Consumers in Respect of Distance Contracts,[98] the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,[99] the Directive on the Legal Protection of Databases,[100] and the Directive on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market.[101]

The Electronic Signatures Directive is made up of fifteen articles and four annexes. The main provisions of this directive are primarily concerned with legal recognition of electronic signatures, free circulation of electronic signature products, liability, technological neutrality, scope, and international aspects.[102]

A. Legal Recognition of Electronic Signatures

Under the Electronic Signatures Directive, an electronic signature cannot be legally discriminated against solely because it is in electronic form.[103] Under Article 2 of the Electronic Signatures Directive, an electronic signature is defined as "data in electronic form which are attached to or logically associated with other

95. *Id.*

96. *Id.*

97. *See* Prof. Dr. jur. M. Lehmann, Dipl.-Kfm., *Electronic Commerce and Consumer Protection in Europe*, 17 SANTA CLARA COMPUTER & HIGH TECH. L.J. 101, 102-05 (2000).

98. Council Directive 97/7/EC, 1997 O.J. (L 144) 19 [hereinafter Distance Contracts Directive].

99. Council Directive 95/46/EC, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive].

100. Council Directive 96/9/EC, 1996 O.J. (L 77) 20 [hereinafter Database Directive].

101. Council Directive 2000/31/EC, 2000 O.J. (L 178) 1 [hereinafter Electronic Commerce Directive].

102. *See* Jacqueline Klosek, *EU Telecom Ministers Approve Electronic Signatures Directive*, 4 CYBERSPACE LAW. 12 (2000).

103. *See id.*

electronic data and which serve as a method of authentication."[104] Under the European model, however, it is important to differentiate between a generic electronic signature and an "advanced electronic signature."[105]

Article 2 sets forth the following requirements for an advanced electronic signature:

(1) it is uniquely linked to the signatory;

(2) it is capable of identifying the signatory;

(3) it is created using means that the signatory can maintain under his sole control; and

(4) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable . . . .[106]

While a generic electronic signature cannot be denied legal effectiveness or admissibility as evidence solely because it is in electronic form, an advanced electronic signature confers an additional benefit.[107] When based on a "qualified certificate," there is a rebuttable presumption that an advanced electronic signature "(a) [satisfies] the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and (b) [is] admissible as evidence in legal proceedings."[108]

The Directive's definition of the term "qualified certificate" refers to certification-service-providers (CSPs).[109] A CSP is an independent party that provides certificates, electronically attesting, through the use of codes or public cryptographic keys, that an electronic signature is linked to a particular person, and verifying the identity of that person.[110] CSPs can also provide services related to electronic signatures, such as the creation and management of electronic signatures for transacting parties.[111]

Annex I of the Electronic Signatures Directive sets forth the

104. Electronic Signatures Directive, *supra* note 2, art. 2(1).

105. *See* Hilary E. Pearson, *E-Commerce Legislation Recent European Community Developments*, 590 PLI/PAT. 373, 383 (2000).

106. Electronic Signatures Directive, *supra* note 2, art. 2(2).

107. *See* Pearson, *supra* note 105, at 384.

108. Electronic Signatures Directive, *supra* note 2, art 5(1).

109. *See id.* art. 2(10).

110. *See id.* art. 2(11).

111. *See id.*

following requirements for a qualified certificate:

Qualified certificates must contain:

(a) an indication that the certificate is issued as a qualified certificate;

(b) the identification of the certification-service-provider and the State in which it is established;

(c) the name of the signatory or a pseudonym, which shall be identified as such;

(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

(e) signature-verification data which correspond to signature-creation data under the control of the signatory;

(f) an indication of the beginning and end of the period of validity of the certificate;

(g) the identity code of the certificate;

(h) the advanced electronic signature of the certification-service-provider issuing it;

(i) limitations on the scope of use of the certificate, if applicable and;

(j) limits on the value of transactions for which the certificate can be used, if applicable.[112]

Annex II goes on to establish the requirements for CSPs:

Certification-service-providers must:

(a) demonstrate the reliability necessary for providing certification services;

(b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;

(c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;

(d) verify, by appropriate means in accordance with national law,

112. *Id.* Annex I.

the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;

(e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;

(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

(h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

(i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purpose of legal proceedings. Such recording may be done electronically;

(j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;

(k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;

(l) use trustworthy systems to store certificates in a verifiable form so that:

- only authorised persons can make entries and changes,
- information can be checked for authenticity,
- certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
- any technical changes compromising these security requirements are apparent to the operator.[113]

B. Free Circulation of Electronic Signature Products

Article 2 defines the term "electronic signature product" as "hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic signature services or are intended to be used for the creation or verification of electronic signatures."[114] Under the Electronic Signatures Directive, all such products and services must be allowed to circulate freely, subject only to the legislation of the country of origin.[115] Also, while Member States may enact legislation regarding domestic certification services such as the establishment of voluntary accreditation schemes, they are not allowed to restrict the provision of certification services that originate in another Member State.[116]

C. Liability

The European framework depends, in large part, on the reliability and integrity of CSPs to maintain an acceptable level of security in transactions that use electronic signatures.[117] Because of the important role they play, CSPs are held liable for damages suffered by any entity or person who reasonably relies on a qualified certificate.[118] Article 6 states that, at a minimum, CSPs are responsible for the following:

113. *Id.* Annex II.
114. *Id.* art. 2(12).
115. *See id.* art. 4(2).
116. *See id.* art. 4(1).
117. *See* Michael & Corral, *supra* note 91.
118. Electronic Signatures Directive, *supra* note 2, art. 6.

(a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;

(b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;

(c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both; unless the certification-service-provider proves that he has not acted negligently.[119]

Such liability can be avoided if the CSP indicates limitations on the use of a qualified certificate that are recognizable to third parties.[120] The CSP will not be held liable for damages caused by transactions in excess of such limitations.[121] Also, the CSP will not be held liable in situations where it can prove that it did not act negligently.[122]

D. Technological Neutrality

Because of the rapid pace at which technology evolves, the Electronic Signatures Directive has been drafted to give recognition to electronic signatures generally, regardless of the particular technology used.[123] It is important that the Directive remain technologically neutral; if it were to prescribe the use of a specific technology, there would be a danger that such technology could become obsolete and the Directive would thus be rendered outdated.[124]

E. Scope

Article 1 suggests that the scope of the Electronic Signatures Directive is intended to be narrow.[125] Its purpose is simply "to facilitate the use of electronic signatures and to contribute to their

119. *Id.* art. 6(1).
120. *See id.* art. 6(3)-(4).
121. *See id.*
122. *See id.* art. 6(2).
123. *See* Klosek, *supra* note 102.
124. *See id.*
125. *See* Electronic Signatures Directive, *supra* note 2, art. 1.

legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market."[126] It is not intended to affect the validity of contracts generally, nor is it meant to modify the formation requirements established by national or European Union contracts law.[127]

Whether the scope of this Directive remains narrow will be determined by a review conducted by the Commission.[128] The review will examine technological, market, and legal developments to determine whether the scope of the Directive should be modified.[129] The Commission will submit its report to the European Parliament and Council by July 19, 2003 at the latest.[130]

F. International Aspects

Article 7 of the Electronic Signatures Directive sets forth provisions intended to encourage the development of electronic commerce on a global scale.[131] These provisions promote electronic commerce by requiring cooperation on the recognition of foreign qualified certificates:[132]

> Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if:
>
> (a) the certification-service-provider fulfills the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State or;
>
> (b) a certification-service-provider established within the Community which fulfills the requirements laid down in this Directive guarantees the certificate; or
>
> (c) the certificate or the certificate-service-provider is recognised

126. *Id.*
127. *Id.*
128. *See id.* art. 12(2).
129. *Id.*
130. *Id.* art. 12(1).
131. *See* Klosek, *supra* note 102.
132. *See id.*

> under a bilateral or multilateral agreement between the Community and third countries or international organisations.[133]

IV. Comparison of American and European Models

It seems clear from the language used in the federal Electronic Signatures Act that "a signature . . . may not be denied legal effect, validity, or enforceability solely because it is in electronic form."[134] Similarly the European Union's Electronic Signatures Directive specifies that "an electronic signature [may not be] denied legal effectiveness . . . solely on the grounds that it is in electronic form."[135] Thus, both laws share a common goal. While both laws confer similar legal recognition on electronic signatures, the approaches taken differ on a number of points. The greatest divergence appears in the areas of scope, consumer protection, and technological neutrality.

A. Scope

One of the most obvious differences between these two laws is in the breath and depth of their influence. Drafted to promote the validity and use of electronic signatures, the Electronic Signatures Act also establishes a framework for electronic negotiable instruments and lays the groundwork for the eventual adoption of UETA by each of the states.[136] In comparison, the scope of the Electronic Signatures Directive is quite narrow; essentially designed to facilitate the use of electronic signatures and related services.[137] Of course, this disparity is understandable since the Electronic Signatures Directive is only one of a series of directives and proposals, each of which addresses a separate issue of electronic commerce.[138]

---

133. Electronic Signatures Directive, *supra* note 2, art. 7(1).

134. Electronic Signatures Act, *supra* note 1, § 101(a)(1).

135. Electronic Signatures Directive, *supra* note 2, art. 5(2).

136. *See* Electronic Signatures Act, *supra* note 1, §§ 102, 201.

137. *See* Electronic Signatures Directive, *supra* note 2, at art. 1.

138. The Distance Contracts Directive, Data Protection Directive, Database Directive, Electronic Commerce Directive, and Electronic Signatures Directive are all intended to benefit the European Union's "Information Society." *See supra* notes 98-101 and accompanying text.

B. Consumer Protection

Both the Electronic Signatures Act and the Electronic Signatures Directive have placed a heavy emphasis on the issue of consumer protection. However, the methods to ensure the security of online transactions differ markedly.

The U.S. model depends on a combination of factors: (1) the strict requirement of consumer consent, (2) a full disclosure to the consumer of his or her rights (i.e., regarding access to written versions of electronic documents, notification of changes to hardware or software requirements to access retained records, and ability to revoke one's consent, etc.), and (3) an access test to confirm the consumer's consent and to demonstrate his or her ability to operate the necessary hardware and software to conduct online transactions.[139] This has the effect of leaving contracting parties in the position to determine the security protocols that are appropriate to national and global electronic commerce.

The European Union model, on the other hand, does not leave the development of security protocols to individual parties. Instead, such protocols are governed by a two-tier system that utilizes advanced electronic signatures and qualified certificates.[140] The security of this system is augmented by a complex network of certification-service-providers, who provide independent authentication and related electronic signature support, thus ensuring that a baseline level of reliability will be maintained.[141]

The benefits of a well-developed system of independent authentication are obvious. Such a system enhances reliability and minimizes uncertainty in online transactions, resulting in more congenial and beneficial relationships between contracting parties. Add to that a clear statement regarding party liability, and the European model seems to have a distinct advantage over the American model, which incorporates neither of these features. However, it should be noted that by allowing electronic commerce to develop according to rules established by the market, the American model offers far greater flexibility.

Also, the European model has endured some criticism regarding its mechanism for recognizing the qualified certificates of foreign

139. *See* Electronic Signatures Act, *supra* note 1, § 101(c)(1).
140. *See* Electronic Signatures Directive, *supra* note 2, art. 5.
141. *See id.* Annex II.

countries.[142] Under this regime, foreign companies that wish to conduct business with the European Union will be forced to seek authentication services from a CSP established in one of the Member States. Alternatively, a foreign company could use a domestic CSP, although it would still have to be "sponsored" by a CSP established in one of the Member States. These options suggest that the European Union does not have much faith in the accreditation systems of other governments.

C. Technological Neutrality

Both the Electronic Signatures Act and the Electronic Signatures Directive recognize the importance of technological neutrality. Both laws define the term "electronic signature" broadly; the American Act describing it as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record,"[143] and the European Directive describing it as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication."[144] Both definitions effectively avoid the dangers posed by mandating the use of a specific technology (i.e., inevitable obsolescence).

However, the European model becomes problematic when it confers additional benefits on "advanced electronic signatures." Parties in the European Union often use "digital signatures" to fulfill the requirements of an advanced electronic signature.[145] A digital signature is a type of electronic signature that uses key-based encryption technology and involves a system of public and private "keys."[146] A digital signature can serve two functions: (1) identify the signer and (2) verify the integrity of the electronic document.[147] Using a private key (that only the signer has access to), the signer's software encrypts the contents of the electronic document, creating a signature unique to that particular document.[148] The receiver of the signed

142. *See id.* art. 7(1).

143. Electronic Signatures Act, *supra* note 1, § 106(5).

144. Electronic Signatures Directive, *supra* note 2, art. 2(1).

145. *See id.* art. 2(2).

146. *See* David M. Nadler & Valerie M. Furman, *Landmark Electronic Signatures Legislation Becomes Effective*, 18 ANDREWS COMPUTER & ONLINE INDUS. LITIG. REP. 13 (2001).

147. *See id.*

148. *See id.*

document uses a public key to decrypt the digital signature and compares the result to the contents of the document.[149] In this manner, if the document has been tampered with, any alterations made to the contents of the document after the signer affixes the digital signature can be detected.[150]

By extending additional benefits to this type of digital signature, the European Union is effectively compelling consumers and other parties to incur additional costs by employing a technology that they might otherwise not have chosen to use. Digital signatures are capable of utilizing strong encryption technology and can provide excellent security benefits. Nonetheless, the European Union is essentially endorsing the use of a specific technology, a policy that directly conflicts with the principle of technological neutrality. While this decision may be convenient and effective in the present, it may yet prove to be immensely costly in the future.

V. Conclusion

It is an unfortunate fact that a global framework for the recognition of electronic signatures does not yet exist—to say nothing of a global framework regarding the conduct of electronic commerce in general. Only when such global frameworks are established will the Internet be able to achieve its full economic and commercial potential. Yet, despite the significant disparity in the approaches taken by the American and European laws on this matter, it is encouraging to note that the United States and the European Union appear willing to coordinate their legislative efforts to converge upon a mutually desirable goal. While these efforts have certainly fallen short of a unified march, they have nonetheless shown an unprecedented level of international cooperation. The next round of legislation, while unlikely to resolve all differences, should nevertheless prove to be both productive and beneficial to all involved.

149. *See id.*
150. *See id.*